PATENT ABSTRACTS OF JAPAN

(11)Publication number : 07-303102
(43)Date of publication of application : 14.11.1995

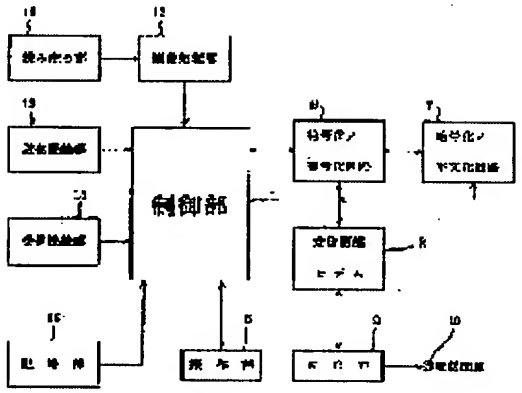
(51)Int.Cl. H04L 9/00
H04L 9/10
H04L 9/12
G09C 1/00
H04K 1/00
H04N 1/44

(21)Application number : 06-095980
(22)Date of filing : 10.05.1994

(71)Applicant : MITA IND CO LTD
(72)Inventor : SHIBATA KOICHI

(54) COMMUNICATION EQUIPMENT

(57)Abstract:
PURPOSE: To prevent the deterioration in the security of a ciphering algorithm resulting from a fact that a head part of an original is generally at a white level by revising a CBC initial value with a prescribed arithmetic operation using number of times of communication for its factor.
CONSTITUTION: An initial setting value IV of CBC ciphering codes in 64-bits decided for each communication opposite party in the case of transmission is read from a RAM in a control section 1 comprising a microcomputer or the like. A read section 11 provided with a scanner reads a transmission original, and ciphering is applied to each block at a head of signals coded by an image processing section 12 by using the initial setting value IV. Ciphering is applied to EXOR processing between succeeding blocks and, e.g. a ciphered text of one-preceding transmission. When the communication is finished, an arithmetic operation of adding, e.g. 1 to the present initial setting value IV and the content of the RAM is rewritten. The result is used for a new initial setting value IV as an understanding with each communication opposite party.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開平7－303102
(43)公開日　平成７年(1995)11月14日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｈ０４Ｌ	9/00				
	9/10				
	9/12				
Ｇ０９Ｃ	1/00		9364－5L		
				Ｈ０４Ｌ　9/00　Ｚ	

審査請求　未請求　請求項の数５　ＯＬ　（全 ９ 頁）　最終頁に続く

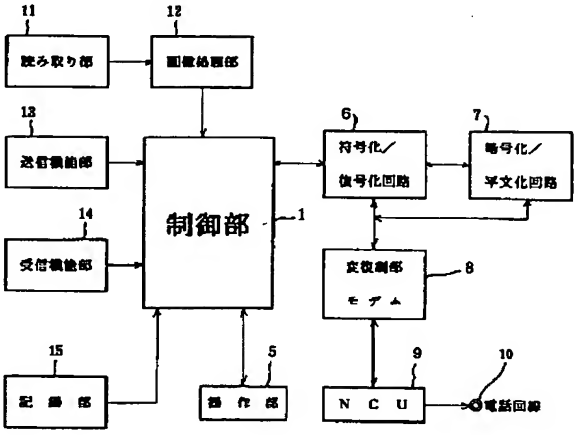
(21)出願番号　特願平6－95980

(22)出願日　平成６年(1994)５月10日

(71)出願人　000006150
三田工業株式会社
大阪府大阪市中央区玉造１丁目２番28号
(72)発明者　柴田　浩一
大阪市中央区玉造１丁目２番28号　三田工業株式会社内
(74)代理人　弁理士　佐野　静夫

(54)【発明の名称】　通信機器

(57)【要約】
【目的】　暗号アルゴリズム強度の低下を効果的に防止する。
【構成】　受信者に対するＣＢＣ初期値の初期設定を行い、ＣＢＣ初期値を算術数字と考えて、送受信者間で暗号通信がなされた場合には、送信側の受信者に対するＣＢＣ初期値ＩＶに１を加えた値に変更し、次回はその変更後の値のＣＢＣ初期値を使用するか、あるいは、暗号通信に際し、送受信者は予め取り決めたテーブルによってＣＢＣ初期値のインデックスから使用するＣＢＣ初期値を決定し、次にカウンタの値を読み出し、先に決定したＣＢＣ初期値の値とカウンタの値を加算し、その算出値をもってＣＢＣ初期値として使用することにより、暗号通信を行う毎に、自動的にＣＢＣ初期値の値を変更する。



1

【特許請求の範囲】

【請求項１】　ＣＢＣモードによる暗号通信を行う通信システムの送受信モデムを構成する通信機器であって、ＣＢＣ初期値を構成する数値を、通信回数を一つの要因とする演算式に基づいて通信の度に前記ＣＢＣ初期値の数値データを変更し、その変更した数値データをそのときの通信時におけるＣＢＣ初期値とする機能を有する暗号通信部を具備していることを特徴とする通信機器。

【請求項２】　ＣＢＣモードによる暗号通信を行う通信システムの送受信モデムを構成する通信機器であって、暗号通信の相手の数だけＣＢＣ初期値が必要な暗号通信機能を有する暗号通信部を備え、且つ、この暗号通信部は、前記ＣＢＣ初期値を算術数字として取り扱い、暗号通信が１回終了する毎に送受信時双方とも、前記ＣＢＣ初期値に所定の演算式を用いて算術演算を施し、次回の暗号通信の際には、前回の暗号通信に基づき前記演算式を用いて行った数値に対応するＣＢＣ初期値を使用するように構成されていることを特徴とする通信機器。

【請求項３】　ＣＢＣモードによる暗号通信を行う通信システムの送受信モデムを構成する通信機器であって、複数のインデックスにそれぞれＣＢＣ初期値の数値データを対応させた秘密暗号テーブルを使用する暗号通信機能を有する暗号通信部を備え、且つ、この暗号通信部は、暗号通信の相手毎に、リセット時からの通信回数を示すカウンタを有し、暗号通信実行時には、前記ＣＢＣ初期値テーブルの指定されたインデックスに対応するＣＢＣ初期値の数値データに対して、前記カウンタが示す数値を加味する所定の演算式を用いて算術演算を施して、そのときのＣＢＣ初期値を設定するように構成されていることを特徴とする通信機器。

【請求項４】　ＣＢＣモードによる暗号通信を行う通信システムの送受信モデムを構成する通信機器であって、通信回数をカウントするカウンタを有し該カウンタのカウント値をＣＢＣ初期値とする機能を有する暗号通信部を具備していることを特徴とする通信機器。

【請求項５】　ファクシミリ装置として構成された請求項１～４のいずれかの通信機器。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、暗号通信機能を有するファクシミリ装置等、秘密暗号通信を行う通信機器に係り、特に暗号通信における秘密性の向上を図った通信機器に関するものである。

【０００２】

【従来の技術】ファクシミリ通信では同一メーカーのファクシミリ装置間での通信に関しては、オプションとして種々の特殊通信を行うことができる。その特殊通信の一つに暗号通信がある。

【０００３】図７はファクシミリ装置における通常の暗号通信の手順を示している。図７（Ａ）において、９１～９４は送信側での信号処理手順であって、送信しようとする原稿は、まず、スキャナ９１によって読み取られる。読み取られた画像データは９２でＭＨ等のデータ圧縮、つまり符号化処理される。次いで、この圧縮された画像データに対して秘密通信とするべく、９３で秘密暗号鍵を用いて暗号化処理が施され、その暗号化データが送信側モデム９４としてのファクシミリ装置から送出される。

2

【０００４】このように従来では、ファクシミリ装置を用いて暗号通信を行う際には、スキャナ９１で読み取った画像データを、そのまま加工を施すことなく、スキャナ９１で読み取った順序に従って暗号化して送信していた。

【０００５】図７(Ｂ)において、９５～９８は受信側での信号処理手順であって、受信側モデム９５としてのファクシミリ装置で受信された原稿の暗号受信データは９６で送信側と同一の秘密暗号鍵を用いて暗号文を解読する、いわゆる平文化処理が施される。平文化された画像データは９７でデータ伸長、つまり復号化され、元の画像データとなり、プリンタ９８により印刷され、これによって受信側で原稿が取り出される。なお、ここで言う秘密暗号鍵は一種のデータである。

【０００６】図８は典型的な送信原稿の一例を示している。なお、図示例の原稿はＣＣＩＴＴ（国際電信電話諮問委員会）の標準原稿である。さて、この原稿Ｍから明らかなように、通常の送信原稿は殆どの部分が“白"つまり文字等が書き込まれていない白地部分で占められている。

【０００７】いま、従来のファクシミリ装置において、スキャナ９１により最初にスキャンされる部分、言い換えれば送信データの最初の部分または、最初に暗号化される部分について考えると、原稿Ｍで最初にスキャンされるのは、その先頭部分Ｈである。通常この先頭部分Ｈは全白であることが多い。このような理由により従来のファクシミリ装置で何らかの原稿を送出しようとする場合は、その送出データの最初の部分は全白に対するデータに対応する可能性が非常に高いと言える。

【０００８】図９はファクシミリ装置における一般的な暗号化処理部の一例として、(Ａ)はＥＣＢモードを用いた例を、また、(Ｂ)はＣＢＣモードを用いた例をそれぞれ示している。図９(Ａ)(Ｂ)に示したいずれの場合も、通常は前述のように、平文Ｐに対して秘密暗号鍵Ｋを用いて暗号文Ｃを出力する。

【０００９】但し、ＥＣＢモードでは図９(Ａ)に示すように、暗号を掛けようとする画像データと暗号が１：１で対応している。これに対し、ＣＢＣモードでは図９(Ｂ)に示すように、例えばｎ番目の平文P_nを暗号化する際、その１回前の暗号文C_{n-1}と平文P_nとのＥＯＲ（排他的論理和）を取り、その結果を暗号化する。なお、この場合、１番目の画像データは暗号文が書かれて

いないため、予め秘密に設定された初期値を用い、この初期値と平文P_1とのＥＯＲを取ることになる。

【００１０】

【発明が解決しようとする課題】このように暗号通信を行う場合、通常、人目に触れるのは暗号文Ｃのみであるので、その暗号が解読される可能性は可成り低いと言える。しかしながら、送信データの最初のスキャン部分は前述のように“全白"に対するデータであることが多い。このため、画像データと暗号が１：１で対応しているＥＣＢモードによるものでは、スキャナ９１で原稿Ｍを読み取らせるとき、受信された暗号化データの始めの部分は“白"を暗号化したものであることが分かってしまい、暗号化アルゴリズムの強度に欠ける。

【００１１】また、ＣＢＣモードでは、初期値は既知ではないため、１番目の画像データが“白"であっても、この“白"を表す平文P_1にもスクランブルが掛けられているため、ＥＣＢモードの場合よりも暗号化アルゴリズムの強度は高いと言えるが、送出データの最初の部分は“白"である点はＥＣＢモードの場合と異なるものではなく、したがって、いずれのモードにおいても、平文Ｐ(全白のデータ)と、それに対する暗号文Ｃが公開されているようなものである。このように従来装置の場合、特定の平文とそれに対する暗号文が既知になるので、この暗号の強度は可成り低下するという問題点があった。

【００１２】本発明は、上記のような問題点に鑑みてなされたもので、ＣＢＣモードによる暗号通信を行う通信システムの送受信モデムを構成する通信機器において、通常原稿の先頭部分が殆どの場合“全白"であること等による暗号アルゴリズム強度の低下を防止するための効果的な対策を施した構成とすることを目的とするものである。

【００１３】

【課題を解決するための手段】上記目的を達成するために本発明では、ＣＢＣ初期値を構成する数値を、通信回数を一つの要因とする演算式に基づいて通信の度に前記ＣＢＣ初期値の数値データを変更し、その変更した数値データをそのときの通信時におけるＣＢＣ初期値とする機能を有する暗号通信部を具備するものとしている。

【００１４】暗号通信部の具体的構成としては、第１に、暗号通信の相手の数だけＣＢＣ初期値が必要な暗号通信機能を有し、且つ、前記ＣＢＣ初期値を算術数字として取り扱い、暗号通信が１回終了する毎に送受信時双方とも、前記ＣＢＣ初期値に所定の演算式を用いて算術演算を施し、次回の暗号通信の際には、前回の暗号通信に基づき前記演算式を用いて行った数値に対応するＣＢＣ初期値を使用するものとしている。

【００１５】また、第２の構成としては、複数のインデックスにそれぞれＣＢＣ初期値の数値データを対応させたＣＢＣ初期値テーブルを使用する暗号通信機能を有し、且つ、暗号通信の相手毎に、リセット時からの通信

回数を示すカウンタを有し、暗号通信実行時には、前記秘密暗号テーブルの指定されたインデックスに対応するＣＢＣ初期値の数値データに対して、前記カウンタが示す数値を加味する所定の演算式を用いて算術演算を施して、そのときのＣＢＣ初期値を設定するものとしている。尚、カウンタのカウント値をそのままＣＢＣ初期値とする構成も可能である。

【００１６】

【作用】上記構成によると、受信者に対するＣＢＣ初期値の初期設定を行い、ＣＢＣ初期値を算術数字と考えて、送受信者間で暗号通信がなされた場合には、送信側の受信者に対するＣＢＣ初期値を例えば予め取り決めた値を加算する等の演算を行って変更し、次回はその変更後の値のＣＢＣ初期値を使用する。以下同様に、暗号通信を行う毎に、演算を行う。受信側も同様に、送信者から暗号通信を受信する度に、送信者に対するＣＢＣ初期値を変更する演算を行う。

【００１７】また、ＣＢＣ初期値テーブルを利用するものでは、暗号通信に際し、送信側はユーザーに設定されたＣＢＣ初期値のインデックスにより、使用するＣＢＣ初期値を決定し、次に、カウンタの値を読み出し、先に決定したＣＢＣ初期値の値とカウンタの値を例えば加算するような算術演算を行う。そして、暗号通信にはその演算によって得られた値をＣＢＣ初期値として使用する。受信側も同様な処理を行う。

【００１８】

【実施例】以下、本発明の実施例を図面を参照しながら説明する。ＣＢＣモードによる暗号通信を行う通信システムの送受信モデムを構成するファクシミリ装置に適用した実施例を図面を参照しながら説明する。図１は本発明の第１実施例に係るファクシミリ装置の全体構成をブロック図で示している。

【００１９】この図において、１はマイクロコンピュータ等からなる制御部であって、全体の制御を司る。この制御部１は図２に示すように、ＣＰＵ２、プログラムＲＯＭ３、ＲＡＭ４等から構成されている。また、ＲＡＭ４は暗号通信を行うときのワーク領域、メモリ領域の一つの形態としての暗号鍵記憶領域、ＣＢＣ初期値（ＩＶ）記憶領域、カウンタ等を有している。

【００２０】図１に戻って、５は操作部、６は符号化／復号化回路、７は当該ファクシミリ装置が送信側として動作するときは、暗号化を行い、受信側として動作するときは平文化を行う暗号化／平文化回路、８は変復調部モデム、９はＮＣＵ（網制御装置）、１０は公衆電話回線である。１１は原稿を読み取るスキャナ１１ａを有する読み取り部である。１２は読み取った画像データにシェーディング補正等の処理を施す画像処理部である。１３は送信機能部、１４は受信機能部、１５はプリント部１５ａ等を有する記録部である。

【００２１】上述した操作部５、変復調部モデム８及び

ＮＣＵ９、スキャナ１１ａ、プリント部１５ａ、リアルタイムクロック１６とＣＰＵ２とは図２に示すように、データバス１６を通して接続されており、ＣＰＵ２を中心とする上記各構成は、以下に述べるように、原稿を正方向及び逆方向で暗号化する暗号通信部として機能するものであり、送受信双方とも、暗号通信としてのプロセスが制御部１においてプログラムされている。

【００２２】次に、上記構成が暗号通信部として機能する場合について、送信側として動作するときの制御部１の動作例を図３のフローチャートを参照しながら説明する。本実施例ではＣＢＣモードの初期値を使用して、秘密暗号鍵を通信毎に変化させる方法を示す。この場合、ＣＢＣモードを利用しているため、先頭のブロック(ここでは６４ビット)のみ全白対応をすればよい。すなわち、ＣＢＣ初期値は通常、６４ビット程度の２進数の数値データである。

【００２３】まず、暗号通信を行う送受信者は共に本実施例装置を使用しているものとする。本実施例では送信者が暗号通信しようとする相手に対し、各々の相手固有のＣＢＣ初期値が存在するような方式を考える。したがって、この場合、暗号通信しようとする相手の数だけＣＢＣ初期値が存在することになる。

【００２４】図３において、送信者が送信動作を開始し、ステップ＃１０５で通信相手に対応するＣＢＣ初期値ＩＶをＲＡＭ４のＣＢＣ初期値記憶領域から読み出す。ここでは、受信者に対するＣＢＣ初期値をＩＶとする。なお、この初期設定値ＩＶは前述のとおり６４ビットの２進数であり、例えば“0000000000000000”等の形で表される。次いで、ステップ＃１１０で、スキャナ１１ａで読み取られた送信原稿を符号化し、さらにステップ＃１１５で、符号化された原稿を前記ＣＢＣ初期値ＩＶにより暗号化する等の通信手順が行われ、ステップ＃１２０で最終的に送信動作が行われる。

【００２５】送信後は、ＣＢＣ初期値ＩＶの変更が行われる。本実施例では、ＣＢＣ初期値の数値データを算術数字として取り扱う。そして、暗号通信が１回終了する毎に、ＣＢＣ初期値に所定の演算式を用いて算術演算を施し、次回の暗号通信の際には、前回の暗号通信に基づき前記演算式を用いて行った数値に対応するＣＢＣ初期値を使用する。この演算式は、ＩＶ’＝ＩＶ＋１で表される。

【００２６】したがって、送受信者間で暗号通信がなされた後は、ステップ＃１２５で送信側の受信者に対するＣＢＣ初期値を“ＩＶ”から“ＩＶ＋１”に変更し、次回はこの“ＩＶ＋１”を特定の相手に対するＣＢＣ初期値として使用するべく、ステップ＃１３０で新たにＩＶ’をＣＢＣ初期値としてＲＡＭのＣＢＣ初期値記憶領域に格納する。

【００２７】以下同様に、暗号通信を行う毎に、ＣＢＣ初期値の値に“１”を足し算する。受信側も同様に、送信者から暗号通信を受信する度、送信者に対するＣＢＣ初期値に“１”を足す。なお、本実施例では、例題としてＣＢＣ初期値に“１”を足す演算を示したが、他の数式による算術演算を用いるようにしてもよい。

【００２８】図４は本実施例装置が受信側として動作するときの制御部１の動作例を示している。受信側においては、受信後、ステップ＃２０５で通信相手に対応するＣＢＣ初期値ＩＶをＲＡＭ４のＣＢＣ初期値記憶領域から読み出す。次いで、ステップ＃２１０で受信データを一旦、ＲＡＭ４へ格納する等の所定手順の受信動作を行った後、ステップ＃２１５で先に読み出したＣＢＣ初期値ＩＶで受信原稿の平文化を行い、さらにステップ＃２２０でそれを復号化し、受信を完了する。

【００２９】この後、受信側においても、ステップ＃２２５で送信側の受信者に対するＣＢＣ初期値を“ＩＶ”から“ＩＶ＋１”に変更し、次回はこの“ＩＶ＋１”を特定の相手に対するＣＢＣ初期値として使用するべく、ステップ＃２３０で新たにＩＶ’をＣＢＣ初期値としてＲＡＭのＣＢＣ初期値記憶領域に格納する。

【００３０】このように本発明の第１実施例では、暗号通信が１回終了する毎に送受信時双方とも、ＣＢＣ初期値に所定の演算式を用いて算術演算を施し、次回の暗号通信の際には、前回の暗号通信に基づき前記演算式を用いて行った数値に対応するＣＢＣ初期値を使用するものであるため、ＣＢＣ初期値を暗号通信しようとする相手の数だけ登録すれば、通信の相手毎に秘密暗号鍵を変更することが可能になるため、暗号強度アップの点で有利であると言える。

【００３１】図５及び図６は、本発明の第２実施例における制御部１の送信動作(図５)と、受信動作(図６)の流れを示している。なお、本実施例の構成は、図１及び図２に示した上記第１実施例のそれと共通しているので、共通の構成についてはその説明を省略する。

【００３２】本実施例においては、送信者が暗号通信しようとする相手に対し、下記表１に示すようなＲＡＭ４のＣＢＣ初期値テーブルを使用する。このＣＢＣ初期値テーブルは、ＣＢＣ初期値を適宜数登録し、それぞれのＣＢＣ初期値としての数値データ毎にインデックスを施したものであって、実際の使用に際しては、ＣＢＣ初期値そのものではなく、インデックスを用いる。したがって、暗号通信の相手の数だけＣＢＣ初期値が存在するわけではなく、相手によっては、他の相手と同じＣＢＣ初期値を使用する可能性もある。なお、該ＣＢＣ初期値テーブルは機器製造時において、ユーザーに対して予め設定しておくものとする。

【００３３】

【表１】

7　　8

インデックス	ＣＢＣ初期値
００	０００００００００００００００
０１	０１２３４５６７８９ＡＢＣＤＥＦ
０２	２２２２２２２２２２２２２２２２
０３	ＦＥＤＣＢＡ９８７６５４３２１０
０４	１１１１１２２２２２３３３３３５
０５	１１２２３３４４５５６６７７８８

【００３４】また、送受信双方の制御部１には暗号通信の相手毎に、リセット時からの特定の送受信者間の通信回数を示すカウンタがソフト的に設けられている。なお、実際には、暗号通信する相手の数だけ、このカウンタが必要になる。いま、このカウンタが示す値を“Ｃ”とする。

【００３５】そして、暗号通信に際し、送信側は図５に示すように、暗号通信を実行するために送信を開始した後、ステップ＃３０５でＣＢＣ初期値テーブルから指定されたインデックスを読み出し、使用するＣＢＣ初期値を決定する。この場合、表１を参照して、例えばインデックスが“０５”と指定されているとすると、“1122334455667788”を選択することになる。いま、このＣＢＣ初期値の値を“ＩＶ”とする。

【００３６】次いで、ステップ＃３１０で通信相手に対応したカウンタの値Ｃを読み出す。、この送信に際しては、ＣＢＣ初期値ＩＶの変更が行われる。本実施例においても、ＣＢＣ初期値の数値データを算術数字として取り扱う。すなわち、指定されたインデックスに対応するＣＢＣ初期値の値ＩＶに対して、カウンタが示す数値Ｃを加味する所定の演算式を用いて算術演算を施し、その算出値ＩＶ’をそのときのＣＢＣ初期値の値とする。この演算式は、ＩＶ’＝ＩＶ＋Ｃで表される。したがって、例えば特定の相手との通信回数が１０回目であるとすれば、カウンタの値Ｃが１０であるから、そのときの送受信者双方のＣＢＣ初期値の値ＩＶ’は“1122334455667798”となる。

【００３７】次いで、ステップ＃３１５で送信画像（原稿）の符号化を行い、ステップ＃３２０で所定手順で送信動作を行う。このとき暗号通信には前記“ＩＶ＋Ｃ”をＣＢＣ初期値として使用する。なお、本実施例においても、ＣＢＣ初期値を決定する算術演算は上記とは異なる数式を用いるようにしてもよい。

【００３８】そして、送信後、ステップ＃３２５で暗号通信が１回終了する毎に、使用したカウンタの値に１を足し算し、ステップ＃３３０でこれによって得られた値Ｃ’（Ｃ＋１）を、ＲＡＭ４のＣＢＣ初期値記憶領域に格納しておく。次回の暗号通信の際には、改めてＣＢＣ初期値テーブルから指定したインデックスを読み出し、使用するＣＢＣ初期値を決定するとともに、カウンタの値としてＣ’を用いることになる。このため、例え続けて同じインデックスを指定したとしても、ＣＢＣ初期値のデータは異なる値となるので、秘密暗号鍵の暗号強度が低下することはない。

【００３９】図６は本実施例装置が受信側として動作するときの制御部１の動作例を示している。受信側においては、受信後、ステップ＃４０５で通信相手と対応するＣＢＣ初期値テーブルのインデックスを読み出し、使用するＣＢＣ初期値を決定し、次いで、ステップ＃４１０で通信相手に対応したカウンタの値Ｃを読み出す。そして、送信側と同じＣＢＣ初期値、すなわち“ＩＶ＋Ｃ”を暗号鍵として受信データの平文化を行い、ステップ＃４２０で受信原稿の復号化を行い、受信を完了する。

【００４０】この後、受信側においても、ステップ＃４２５で送信側の受信者に対するカウンタの値を“Ｃ”から“Ｃ＋１”に変更し、ステップ＃４３０で得られた値Ｃ’（Ｃ＋１）をＲＡＭ４のＣＢＣ初期値記憶領域に格納する。

【００４１】このように本発明の第２実施例では、暗号通信実行時には予め設定された秘密暗号テーブルの指定されたインデックスに対応するＣＢＣ初期値の数値データに対して、カウンタが示す数値を加味する所定の演算式を用いて算術演算を施すことにより、そのときのＣＢＣ初期値を設定するようにしており、ＣＢＣ初期値を相手の数だけ準備しなくてもよいため、暗号通信を前記第１実施例よりも簡単に行うことができる。

9

【００４２】次に、本発明の第３の実施例は、ＣＢＣ初期値として通信回数をカウントするカウンタの値を、そのまま使う。送信側と受信側のカウンタは通信回数をカウントする。そのカウント値は前記ＣＢＣ初期値ＩＶとして使用される。この第３実施例では、カウンタの値をそのまま初期値として使用するので、他に初期値を用意しておいたり、算術演算を施したりする必要がないというメリットがある。

【００４３】

【発明の効果】以上説明したように本発明によるときは、ＣＢＣ初期値を構成する数値を、通信回数を一つの要因とする演算式に基づいて通信の度に前記ＣＢＣ初期値の数値データを変更し、その変更した数値データをそのときの通信時におけるＣＢＣ初期値とする機能を有するものとしているので、ＣＢＣモードによる暗号通信を行う場合、送信データ量を全く変化させず送信することができるものでありながら、平文と暗号文のペアが既知とならず、暗号の強度が低下することがない。

【００４４】すなわち、本発明では、秘密暗号鍵の変更のために必要な演算を機器が自動的に行い、且つ、その演算結果に基づきＣＢＣ初期値のデータを自動的に変更していくので、ユーザーは簡単な操作でもって高度な暗号強度を有する暗号通信を実現することができる。

【００４５】また、暗号通信部の具体的構成として、請求項２ではＣＢＣ初期値を算術数字として取り扱い、暗号通信が１回終了する毎に送受信時双方とも、前記ＣＢＣ初期値に所定の演算式を用いて算術演算を施し、次回の暗号通信の際には、前回の暗号通信に基づき前記演算式を用いて行った数値に対応するＣＢＣ初期値を使用するものとしているので、ＣＢＣ初期値を暗号通信しようとする相手の数だけ登録すれば、通信の相手毎にＣＢＣ初期値を変更することが可能になるため、暗号強度アップの点で有利なものとなる。

【００４６】さらに、請求項３では暗号通信の相手毎にリセット時からの通信回数を示すカウンタを有し、暗号通信実行時には、前記秘密暗号テーブルの指定されたインデックスに対応するＣＢＣ初期値の数値データに対して、前記カウンタが示す数値を加味する所定の演算式を用いて算術演算を施して、そのときのＣＢＣ初期値を設定するものとしているので、ＣＢＣ初期値を相手の数だけ準備しなくてもよく、したがって暗号通信を請求項２のものよりも更に簡単に行うことができる。

【００４７】また、請求項４では、ＣＢＣ初期値として通信回数をカウントするカウンタの値をそのまま初期値として使用するので、他に初期値を用意しておいたり、

10

算術演算を施したりする必要がない。

【００４８】そのうえ、上記したいずれの構成においても、例えばエラーの発生等により同じ原稿が繰り返し送信されることがあっても、先頭の画像データはその送信時毎に異なるので、暗号強度が一層高まり、例えば通常原稿の先頭部分が殆どの場合“全白”であることによる暗号アルゴリズム強度の低下を効果的に防止することができる。

【図面の簡単な説明】

【図１】　本発明の第１実施例に係るファクシミリ装置の構成を示す概略ブロック図。

【図２】　その制御部を具体的にするとともに他の構成部分との接続状態を示すブロック図。

【図３】　制御部の送信に関する動作例を示すフローチャート。

【図４】　同制御部の受信に関する動作例を示すフローチャート。

【図５】　本発明の第２実施例に係るファクシミリ装置における制御部の送信に関する動作例を示すフローチャート。

【図６】　同制御部の受信に関する動作例を示すフローチャート。

【図７】　一般的なファクシミリ装置における通常の暗号送信の手順を示すブロック図。

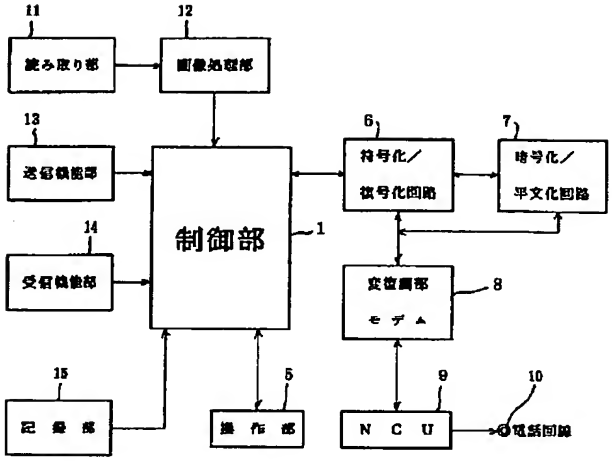
【図８】　送信原稿の一例を示す平面図。

【図９】　一般的なファクシミリ装置における暗号化処理部の一例を示すブロック図。

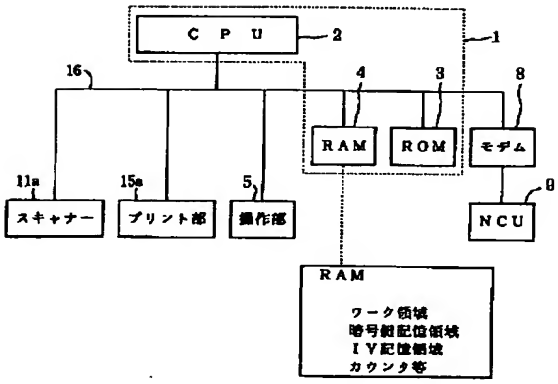
【符号の説明】

１　制御部
２　ＣＰＵ
３　ＲＯＭ
４　ＲＡＭ
５　操作部
６　符号化／復号化回路
７　暗号化／平文化回路
８　変復調部モデム
９　ＮＣＵ
１１　読み取り部
１１ａ　スキャナ
１２　画像処理部
１３　送信機能部
１４　受信機能部
１５　記録部
１５ａ　プリント部

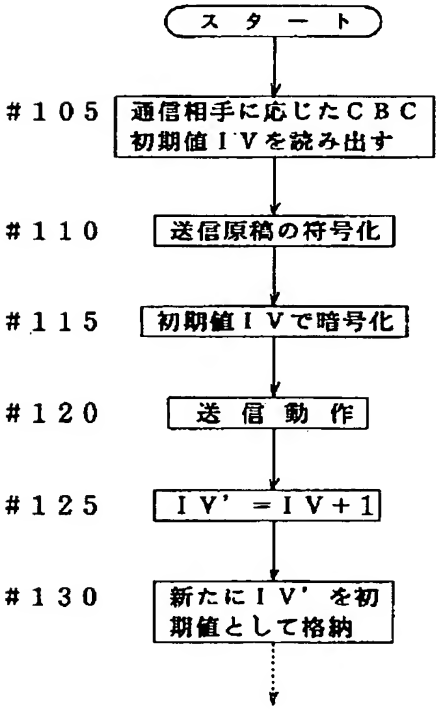
【図１】


11
読み取り部
12
画像処理部
13
送信機能部
制御部
1
6
符号化／復号化回路
7
暗号化／平文化回路
14
受信機能部
変復調部
モデム
8
15
記録部
5
操作部
9
NCU
10
電話回線

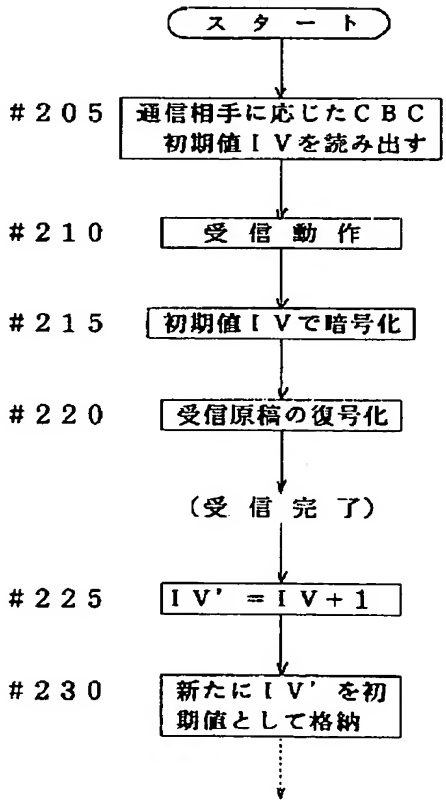
【図２】


CPU
2
1
16
4
3
8
RAM
ROM
モデム
11a
スキャナー
15a
プリント部
5
操作部
9
NCU
RAM
ワーク領域
暗号鍵記憶領域
ＩＶ記憶領域
カウンタ等

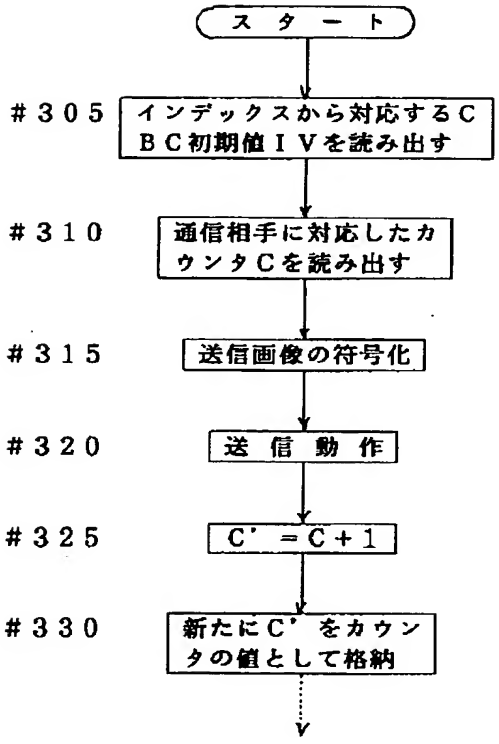
【図３】


スタート
＃１０５
通信相手に応じたＣＢＣ初期値ＩＶを読み出す
＃１１０
送信原稿の符号化
＃１１５
初期値ＩＶで暗号化
＃１２０
送信動作
＃１２５
ＩＶ'＝ＩＶ＋１
＃１３０
新たにＩＶ'を初期値として格納

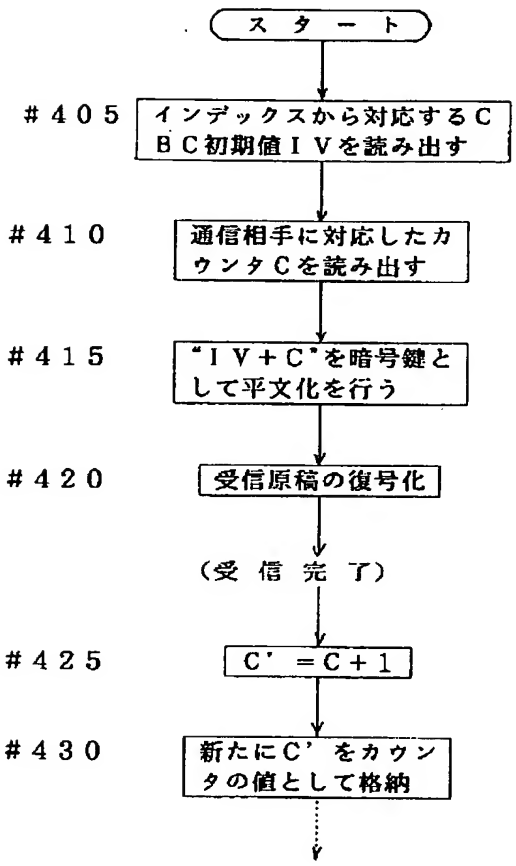
【図４】


スタート
＃２０５
通信相手に応じたＣＢＣ初期値ＩＶを読み出す
＃２１０
受信動作
＃２１５
初期値ＩＶで暗号化
＃２２０
受信原稿の復号化
（受信完了）
＃２２５
ＩＶ'＝ＩＶ＋１
＃２３０
新たにＩＶ'を初期値として格納

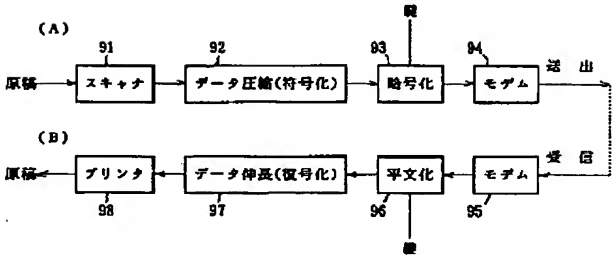
【図５】


スタート
#３０５
インデックスから対応するＣＢＣ初期値ＩＶを読み出す
#３１０
通信相手に対応したカウンタＣを読み出す
#３１５
送信画像の符号化
#３２０
送信動作
#３２５
C'＝C＋１
#３３０
新たにC'をカウンタの値として格納

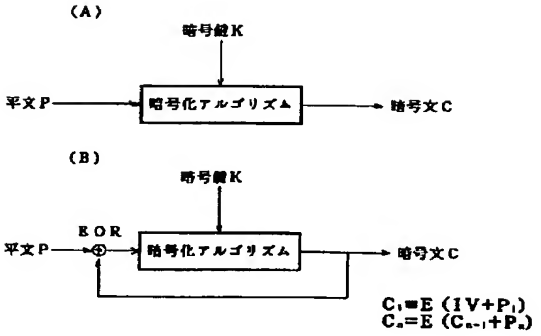
【図６】


スタート
#４０５
インデックスから対応するＣＢＣ初期値ＩＶを読み出す
#４１０
通信相手に対応したカウンタＣを読み出す
#４１５
"ＩＶ＋Ｃ"を暗号鍵として平文化を行う
#４２０
受信原稿の復号化
（受信完了）
#４２５
C'＝C＋１
#４３０
新たにC'をカウンタの値として格納

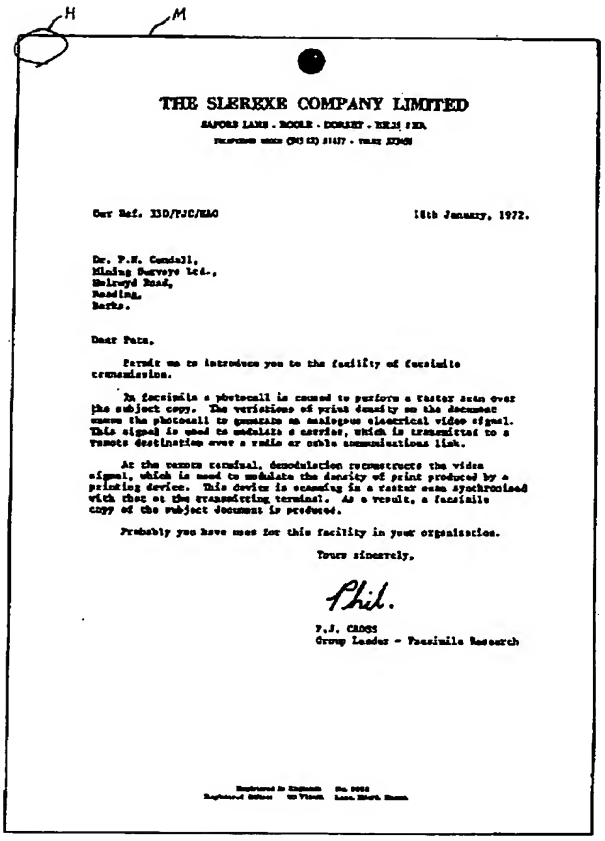
【図７】


(A)
91
92
93
94
原稿
スキャナ
データ圧縮(符号化)
暗号化
モデム
送出
鍵
(B)
原稿
プリンタ
データ伸長(復号化)
平文化
モデム
受信
98
97
96
95
鍵

【図９】


(A)
暗号鍵K
平文P
暗号化アルゴリズム
暗号文C
(B)
暗号鍵K
EOR
平文P
暗号化アルゴリズム
暗号文C
C₁=E (IV+P₁)
Cₙ=E (Cₙ₋₁+Pₙ)

【図８】



THE SLEREXE COMPANY LIMITED

SAFORD LANE . BOOLE . DORSET . BH25 8ER

Our Ref. XSD/PJC/EAG 18th January, 1972.

Dr. P.W. Cundall,
Mining Surveys Ltd.,
Holroyd Road,
Reading,
Berks.

Dear Pete,

Permit me to introduce you to the facility of facsimile transmission.

In facsimile a photocell is caused to perform a raster scan over the subject copy. The variations of print density on the document causes the photocell to generate an analogous electrical video signal. This signal is used to modulate a carrier, which is transmitted to a remote destination over a radio or cable communications link.

At the remote terminal, demodulation reconstructs the video signal, which is used to modulate the density of print produced by a printing device. This device is scanning in a raster scan synchronised with that at the transmitting terminal. As a result, a facsimile copy of the subject document is produced.

Probably you have uses for this facility in your organisation.

Yours sincerely,

Phil.

P.J. CROSS
Group Leader - Facsimile Research

フロントページの続き

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｈ０４Ｋ	1/00		Ｚ		
Ｈ０４Ｎ	1/44				